

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

05 NOV 15 PM 2:41

TERESA HENDRICKS, individually)
and on behalf of a class)
)
Plaintiff,)
v.)
)
DSW SHOE WAREHOUSE INC.,)
an Ohio Corporation)
)
Defendant.)

1:05 CV 0767
Wendell A. Miles
Senior, U.S. District Judge

JURY TRIAL DEMANDED

COMPLAINT – CLASS ACTION

MATTERS COMMON TO MULTIPLE CLAIMS

INTRODUCTION

1. Plaintiff brings this action to secure redress from the failure of defendant DSW, Inc., ("DSW"), to comply with its undertaking to use private financial information provided to it by its customers for the sole purpose of facilitating transactions with those customers, and to safeguard such information, with the result that it was compromised.

JURISDICTION AND VENUE

2. This Court has jurisdiction under 28 U.S.C. §1332.
3. Venue in this District is proper in that DSW does business in this District and in that the personal information that gave rise to the violations of law complained of was received by DSW in this District.

PARTIES

4. Plaintiff Teresa Hendricks is an individual who resides in Grand Rapids, Michigan.

5. Defendant DSW is an Ohio corporation with principal offices at 4150 East 5th Avenue, Columbus, Ohio 43219. Its registered agent and office are CSC-Lawyers Incorporating Service (Company), 601 Abbott Rd., East Lansing, Michigan 48823.

6. DSW operates approximately 198 shoe stores throughout the United States, of which at least 3 are located in the Western District of Michigan:

- a. 3665 28th Street SE., Grand Rapids, Michigan 49512.
- b. 2800 Town Center Blvd., Lansing, Michigan 48912.
- c. 5119 West Main Street, Kalamazoo, Michigan 49009.

FACTS

Compromise of Personal Information Held by DSW

7. In late 2004 to early 2005, DSW's customers' personal financial information from 108 of DSW's store locations was compromised. This included at least seven Michigan DSW locations:

- a. Ann Arbor, Michigan,
- b. Dearborn, Michigan,
- c. Lansing, Michigan,
- d. Novi, Michigan,
- e. Sterling Heights, Michigan,
- f. Troy, Michigan, and
- g. West Bloomfield, Michigan.

8. The information compromised included (a) the numbers and the names associated with approximately 1.4 million credit and debt cards and (b) 96,000 checking account numbers (Magnetic Ink Character Recognition "MICR" numbers) and the drivers' license

numbers provided by check writers.

9. According to DSW's filings with the Securities & Exchange Commission the data was compromised over a two week period. DSW Form S-1A, filed June 27, 2005, p. 4

10. About the first week of March 2005, DSW became aware that the above mentioned personal information was compromised.

11. On March 10, 2005, the Ohio Attorney General urged DSW to "take responsibility and contact all Ohio consumers possible affected" by the unauthorized access of DSW's patrons' personal information.

12. On April 20, 2005, Michigan Attorney General stated, "Since discovering the security breach last month, my office has been in communication with DSW to ensure Michigan consumers effected by the security breach receive timely and through information[.]"

13. On April 22, 2005, the Ohio Attorney General stated, "We see no reason why DSW, working with the credit card companies and the underlying issuing banks, cannot arrange for direct notification of every affected consumer."

14. DSW declined to do so voluntarily.

15. On June 6, 2005, the Ohio Attorney General filed suit against DSW under the Ohio Consumer Sales Practices Act, O.R.C. 1345.01 *et seq*, requesting that the court, "ORDER Defendant [DSW] to individually notify each and every consumer who had personal information stolen from Defendant's custody and control, in writing, that their personal information was stolen from Defendant's custody and control".

16. On or about June 2005, plaintiff received a letter from DSW advising her that she was one of the customers whose information had been stolen.

DSW's Obligation to Protect Information

17. At all times relevant herein, DSW was an authorized Visa® Merchant authorized by Visa® U.S.A. to accept Visa® credit and debit cards and an authorized MasterCard® Merchant authorized by MasterCard® International to accept MasterCard® credit and debit cards for the payment of personal goods.

18. Visa® U.S.A. (“Visa”) is a privately-held for profit association that supplies and supports Visa® credit and debit cards issued by financial institutions to its customers by providing an authorization service for Visa® card transactions and a clearing and settlement service to transfer payment information between parties involved in credit and debit card transactions.

19. DSW accepts Visa® credit and debit cards, and other debit and credit cards, such as MasterCard®, issued from other organizations, from consumers for payment of their purchases.

20. On information and belief, Visa®’s Operating Regulations include provisions designed to protect the security of cardholder information (“Visa® Cardholder Security Program” or “VCSP”).

21. On information and belief, DSW is under contractual obligation, as a condition of being permitted to process transactions through the Visa® network, to comply with the Visa®’s Operating Regulations and the VCSP.

22. On information and belief, the Visa® Operating Regulations expressly prohibit DSW from disclosing any Visa® cardholder account numbers, magnetic stripe information, or transaction information to unauthorized third parties.

23. On information and belief, the Visa® Operating Regulations expressly

prohibit DSW from retaining or storing any Visa® card magnetic stripe information after the authorization of a credit card transaction.

24. On information and belief, the Visa® Operating Regulations and the VCSP expressly require DSW to properly secure and protect Visa® cardholder information and magnetic stripe data from unauthorized disclosure or access.

25. On information and belief, other credit card and debit service organizations, such as those that facilitate transactions engaged in with MasterCard®, Discover®, and American Express® cards, impose the same or similar on DSW as Visa®.

26. On information and belief, on or before October 31, 2004, DSW received a letter from one or more companies: American Express®, Diners Club®, Discover® Card, JCB®, MasterCard® International or Visa® U.S.A., informing DSW of DSW's requirements for Securing Cardholder Information as follows:

- Do not store the following under any circumstance:
 - Full contents of any track from the magnetic stripe on the back of the card.
 - Card-validation code-the three-digit value printed on the signature panel of a MasterCard®, Visa®, Discovery® Card, JCB®, or Diners Club® card, and four-digit code printed on the front of an American Express® card.
- Store on that portion of the customer's account information that is essential to your business - i.e. name, account number or expiration date.
- Store all materials containing this information (e.g., authorization

logs, transaction reports, transactional receipts, car rental agreements, and carbons) in a secure area limited to authorized personnel.

- *Destroy or purge all media containing obsolete transaction data with cardholder information.* Exhibit A [Emphasis supplied].

Public Understanding As to Use of Credit and Debit Card Information

27. As a result of the Visa® regulations and similar regulations of other credit and debit card issuing organizations, such as MasterCard®, it is the general understanding of the public, and of plaintiff, that merchants such as DSW do not use or permit the use of information obtained from credit and debit cards except to facilitate the transactions in connection with which the cards are presented.

28. It is also the general understanding of the public and of plaintiff that merchants such as DSW take measures to prevent the use of information obtained from credit and debit cards other than to facilitate the transactions in connection with which the cards are presented.

29. Such measures to keep the information secure would include properly and promptly deleting or destroying the information after the merchant has received payment.

DSW's Negligence In Handling Information

30. Rather than deleting or otherwise disposing of the Visa® credit and debit cardholders personal information as required by the Visa® Operating Regulations, DSW retained it.

31. On information and belief, DSW has a contract with Visa® that requires DSW to comply with the Visa® Operating Regulations and the VCSP, that require that

cardholder information not to be improperly retained or disclosed.

32. On information and belief, DSW failed to take reasonable precautions to prevent theft of customer information entrusted to it.

33. On information and belief, DSW, in contravention of the Visa® Operating Regulations and the VCSP, improperly retained Visa® magnetic stripe information subsequent to authorization of transactions.

34. On information and belief, DSW failed to protect and/or secure the Visa® card magnetic strip information that was retained also in contravention of the Visa® Operating Regulations and VSCP.

35. On information and belief DSW improperly retained the information described above during a time period including late 2004 and early 2005.

36. On information and belief, DSW has contractual obligations to protect, secure, and dispose of credit card magnetic strip information with other credit card companies such as MasterCard®, similar to its contractual obligations with Visa®.

Facts Relating to Plaintiff

37. Plaintiff had made purchases of shoes from DSW on a number of occasions during late 2004 and early 2005.

38. Plaintiff had made shoe purchases at both the Lansing, Michigan and Grand Rapids, Michigan locations.

39. Plaintiff paid using a MasterCard® debit card associated with her checking account during late 2004 and early 2005.

40. Plaintiff provided personal information to DSW for the sole purpose of facilitating transactions with DSW and with the understanding that DSW would take appropriate

measures to prevent use of such information for other purposes.

41. As a result of DSW's failure to safeguard and delete her personal information, plaintiff is concerned about identity theft and the misuse of the compromised information.

CLASS ALLEGATIONS

42. Plaintiff brings this action on behalf of a class, consisting of (a) all persons who have Michigan addresses or did business with an Michigan DSW location, (b) whose personal information from either their credit card, debit card, or personal check was retained by DSW (c) and was compromised by a third party.

43. The class is so numerous that joinder of all members is impracticable. The 1.4 million figure in DSW's press release, coupled with the fact that at least 6% of DSW's stores are in Michigan, indicates that 50,000 to 100,000 Michigan residents had their information compromised by an unauthorized third party.

44. There are questions of fact or law common to the class, which common questions predominate over any questions affecting only individual members. The predominant common questions include:

a. Whether DSW breached its contractual obligations to its customers to protect, secure, and properly dispose of its customers' credit card, debit card, and check information;

b. Whether DSW breached its contractual obligations to the credit card and debit card issuers and service organizations to protect, secure, and properly dispose of its customers' credit card, debit card, and check information;

c. Whether plaintiff and the putative class were intended

beneficiaries of DSW's contractual obligations to the credit card and debit card issuers and service organizations;

d. Whether DSW was negligent in protecting consumers' personal information entrusted to it;

h. The appropriate relief.

45. Plaintiff will fairly and adequately protect the interest of the class.

46. A class action is an appropriate method for the fair and efficient adjudication of the controversy, in that individual actions are not economically feasible.

COUNT I – BREACH OF DSW'S CONTRACT WITH ITS CUSTOMERS

47. Plaintiff incorporates paragraphs 1-46.

48. When DSW obtained private information from its customers, it impliedly agreed and undertook to use such information for the sole purpose of facilitating transactions with those customers.

49. DSW breached such agreement and undertaking by failing to safeguard the information and limit its use to the sole purpose of facilitating transactions with customers.

50. DSW's customers have been subjected to increased risk of identity theft and fraudulent use of their information.

51. The risk of identity theft and fraudulent use of information requires DSW's customers to monitor their accounts and credit reports, or cause them to be monitored.

52. As a result, plaintiff and each member of the class has suffered quantifiable loss.

WHEREFORE, plaintiff requests that the Court enter judgment in favor of plaintiff and the class and against DSW for:

- a. Damages in an amount sufficient to pay for the monitoring of credit reports and accounts;
- b. An injunction requiring DSW to take adequate measures to protect consumer data entrusted to it;
- c. Costs of suit;
- d. Such other or further relief as the Court deems proper.

COUNT II – BREACH OF DSW'S CONTRACT WITH CARD ISSUERS

- 53. Plaintiff incorporates paragraphs 1-46.
- 54. Plaintiff and the class members are intended third party beneficiaries of DSW's contracts with Visa®, MasterCard®, American Express®, Discover® and other card issuers and service organizations, which contracts require DSW to secure, protect, and dispose of plaintiff's credit and debit card information.
- 55. DSW breached its contractual obligations by:
 - a. Failing to comply with the Visa Operating Regulations and the VSCP;
 - b. Improperly retaining Visa card magnetic stripe information;
 - c. Failing to protect and secure retained Visa card magnetic stripe information; and
 - d. Allowing access to Visa card magnetic stripe information to unauthorized third parties.

- 56. On information and belief, DSW breached its similar contractual obligations with other credit and debit card issuing organizations, such as MasterCard®.
- 57. DSW's customers have been subjected to increased risk of identity theft

and fraudulent use of their information as a result.

58. The risk of identity theft and fraudulent use of information requires DSW's customers to monitor their accounts and credit reports, or cause them to be monitored.

59. As a result, plaintiff and each member of the class has suffered quantifiable loss.

WHEREFORE, plaintiff requests that the Court enter judgment in favor of plaintiff and the class and against DSW for:

- a. Damages in an amount sufficient to pay for the monitoring of credit reports and accounts;
- b. An injunction requiring DSW to take adequate measures to protect consumer data entrusted to it;
- c. Costs of suit;
- d. Such other or further relief as the Court deems proper.

COUNT III – INDIVIDUAL CLAIM - MICHIGAN CONSUMER PROTECTION ACT

60. Plaintiff incorporates paragraphs 1-46.

61. Plaintiff asserts this claim only on behalf of herself.

62. DSW intended the plaintiff to engage in debit card transactions to facilitate purchases with it.

63. DSW intended plaintiff to rely on DSW to protect the information she furnished in such transactions in such manner that the transactions would be protected, secure, and not susceptible to access or compromise by unauthorized third parties.

64. Protecting personal information furnished in such transactions is a material fact when conducting debit card transactions.

65. DSW did not take appropriate measures to protect plaintiff's information in such manner that it would not be accessed or compromised by an unauthorized third party.

66. DSW failed to disclose this material fact, that it was not implementing adequate security measures with regard to plaintiff's personal information.

67. DSW's non-disclosure deceived plaintiff about the security of her personal information.

68. DSW's failure to take appropriate measures to protect plaintiff's information in such manner that it would not be accessed or compromised by an unauthorized third party is a fact that could not reasonably be known by the plaintiff.

69. DSW failed to promptly contact Plaintiff that her personal information had been compromised by an unauthorized third party.

70. DSW's acts occurred in the course of trade or commerce.

71. DSW thereby engaged in an unfair, unconscionable, or deceptive method, act, or practice in the conduct of trade or commerce in violation of M.C.L. § 445.903(1)(s).

72. The risk of identity theft and fraudulent use of information requires DSW's customers to monitor their accounts and credit reports, or cause them to be monitored.

73. DSW's conduct is the direct and proximate cause of the damage.

WHEREFORE, plaintiff requests that the Court enter judgment in favor of plaintiff and against DSW for:

a. Damages in an amount sufficient to pay for the monitoring of credit reports and accounts or \$250, which ever is greater;

b. An injunction requiring DSW to take adequate measures to protect consumer data entrusted to it;

- c. Attorney's fees, litigation expenses and costs of suit;
- d. Such other or further relief as the Court deems proper.

WHEREFORE, plaintiff requests that the Court enter judgment in favor of plaintiff and the class and against DSW for:

- a. Damages in an amount sufficient to pay for the monitoring of credit reports and accounts;
- b. Damages under the Michigan Consumer Protection Act, that being actual damage or \$250, whichever is greater on her individual claim;
- c. An injunction requiring DSW to take adequate measures to protect consumer data entrusted to it;
- d. Costs of suit;
- e. Such other or further relief as the Court deems proper.



Curtis C. Warner

EDELMAN, COMBS, LATTURNER
& GOODWIN, LLC
By: Curtis C. Warner (P59915)
120 S. LaSalle Street, 18th Floor
Chicago, Illinois 60603
(312) 739-4200
(312) 419-0379 (FAX)

JURY DEMAND

Plaintiff demands a trial by jury. FED. R. CIV. P. 38(b)



Curtis C. Warner